(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－65438

(43)公開日　平成11年(1999)３月５日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｚ
			６１０Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 6 頁）

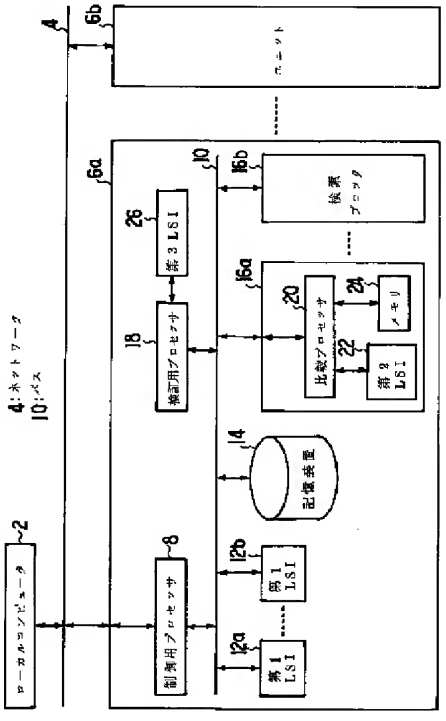
(21)出願番号　特願平9－230562

(22)出願日　平成９年(1997)８月27日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　高橋　勝己
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　飯田　全広
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　暗号強度評価装置

(57)【要約】
【課題】　従来技術で行われた暗号強度評価を行える装置を得ることを目的とする。
【解決手段】　暗号強度評価装置は、各ユニット６ａ，６ｂとこれを制御するローカルコンピュータ２とを有する。各ユニットは、表を生成する第１ＬＳＩ１２ａ，１２ｂと、生成された表を格納する記憶装置１４と、暗号文を加工する第２ＬＳＩ２２と、前記表を取り出して展開するメモリ２４と、前記表と前記暗号文を加工した値とを比較する比較プロセッサ２０と、この比較プロセッサ２０から取り出した値を検証する検証用プロセッサ１８と、検証のために前記表の生成時に用いた初期値を加工する第３ＬＳＩ２６と、これらを制御する制御用プロセッサ８と、を有する。この暗号強度評価装置を使用して、予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求める。



1

【特許請求の範囲】
【請求項１】　暗号文を入手して、その鍵を求める暗号強度評価装置において、
表を生成する第１ＬＳＩと、
生成された表を格納する記憶装置と、
暗号文を加工する第２ＬＳＩと、
前記表を取り出して展開するメモリと、
前記表と、前記暗号文を加工した値と、を比較する比較プロセッサと、
この比較プロセッサから取り出した値を検証する検証用プロセッサと、
検証のために前記表の生成時に用いた初期値を加工する第３ＬＳＩと、
前記第１ＬＳＩ、前記記憶装置、前記第２ＬＳＩ、前記メモリ、前記比較プロセッサ、前記検証用プロセッサ及び前記第３ＬＳＩを制御する制御用プロセッサと、を有するユニットと、
このユニットを制御するローカルコンピュータと、を有し、
予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めることを特徴とする暗号強度評価装置。
【請求項２】　前記第１ＬＳＩ、前記第２ＬＳＩ及び前記第３ＬＳＩを１つのＬＳＩで実現することを特徴とする請求項１に記載の暗号強度評価装置。
【請求項３】　前記メモリは連想記憶メモリであり、前記比較プロセッサは、前記連想記憶メモリが一致した値があったと判定した場合、その値を取り出す回路で構成されることを特徴とする請求項１又は２に記載の暗号強度評価装置。
【請求項４】　前記回路を前記第２ＬＳＩに付加することを特徴とする請求項３に記載の暗号強度評価装置。
【請求項５】　前記第１ＬＳＩ、前記第２ＬＳＩ及び前記第３ＬＳＩは、強度評価する暗号を変更することができることを特徴とする請求項１～４のうち、いずれか１項に記載の暗号強度評価装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号強度評価装置、特に予め平文を想定し、暗号文に対応する鍵を探索することにより、暗号強度を評価する暗号強度評価装置に関する。
【０００２】
【従来の技術】従来の暗号方式として、米国の標準暗号である秘密鍵暗号方式ＤＥＳ（DataEncryption Standard)等が知られている。この暗号方式では、平文をある一定のブロックに区切り、ブロック単位で秘密鍵によって暗号化することにより、平文全体を暗号化することを特徴とする。この方式の暗号強度、即ち、解読のされにくさは非常に高いとされるが、処理をブロック単位で行うため、平文の種類によっては、ブロック毎に一定の統計的性質を示す場合があり、これが、暗号強度を低下させる原因になる。また、暗号強度については、現在のところ特に定まった基準はなく、開発段階である。

2

【０００３】従来の暗号強度評価については、『M.E.Hellman, "A cryptanalytic time-memory trade-off", IEEE Transaction on Infomation Theory, Vol.IT-26 No.4』（以下、従来技術という）において記載された技術がある。この技術においては、予め平文から表を作成し、暗号文を加工しつつ、表との比較を繰り返すことにより、暗号強度を評価している。
【０００４】
【発明が解決しようとする課題】しかしながら、上述の従来技術は、暗号強度の評価方法の技術を単に提示したに留まり、上記暗号強度評価方法を実現することができず、特に従来開示された評価方法をそのまま具体化すると、装置が大型、高価となり、また評価時間が長くなってしまうという問題があった。
【０００５】本発明は以上のような問題点を解決するためになされたものであり、その目的は、従来技術で行われた暗号強度評価を行える装置を得ることを目的とする。
【０００６】
【課題を解決するための手段】以上のような目的を達成するために、第１の発明に係る暗号強度評価装置は、暗号文を入手して、その鍵を求める暗号強度評価装置において、表を生成する第１ＬＳＩと、生成された表を格納する記憶装置と、暗号文を加工する第２ＬＳＩと、前記表を取り出して展開するメモリと、前記表と、前記暗号文を加工した値と、を比較する比較プロセッサと、この比較プロセッサから取り出した値を検証する検証用プロセッサと、検証のために前記表の生成時に用いた初期値を加工する第３ＬＳＩと、前記第１ＬＳＩ、前記記憶装置、前記第２ＬＳＩ、前記メモリ、前記比較プロセッサ、前記検証用プロセッサ及び前記第３ＬＳＩを制御する制御用プロセッサと、を有するユニットと、このユニットを制御するローカルコンピュータと、を有し、予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めるものである。
【０００７】第２の発明に係る暗号強度評価装置は、第１の発明において、前記第１ＬＳＩ、前記第２ＬＳＩ及び前記第３ＬＳＩを１つのＬＳＩで実現するものである。
【０００８】第３の発明に係る暗号強度評価装置は、第１又は第２の発明において、前記メモリは連想記憶メモリであり、前記比較プロセッサは、前記連想記憶メモリが一致した値があったと判定した場合、その値を取り出す回路で構成されるものである。

【０００９】第４の発明に係る暗号強度評価装置は、第３の発明において、前記回路を前記第２ＬＳＩに付加するものである。

【００１０】第５の発明に係る暗号強度評価装置は、第１～４の発明うち、いずれか１つの発明において、前記第１ＬＳＩ、前記第２ＬＳＩ及び前記第３ＬＳＩは、強度評価する暗号を変更することができるものである。

【００１１】

【発明の実施の形態】以下、図面に基づいて本発明の好適な実施の形態について説明する。この際、ＤＥＳ暗号を用いて暗号強度の評価を行う暗号強度評価装置について説明する。

【００１２】実施の形態１．図１は、本発明の実施の形態１である暗号強度評価装置を示すブロック図である。暗号強度評価装置は、ローカルコンピュータ２と、ユニット６ａ，６ｂと、ユニット６ａ，６ｂとローカルコンピュータ２との間に接続されたネットワーク４と、を有する。

【００１３】ローカルコンピュータ２は、装置全体の管理やユーザーとのインターフェイスを行う。ユニット６ａ，６ｂは、ローカルコンピュータ２からの指示により各処理を行うＬＳＩ等をまとめたものである。ネットワーク４は、データの送受信を行う。なお、各ユニット６ａ，６ｂは、ローカルコンピュータ２と並列接続されている。また、ユニットは図１に示す２個に限定されず、複数個ローカルコンピュータ２と並列接続されていてもよい。

【００１４】各ユニット６ａ，６ｂは、ローカルコンピュータ２とネットワーク４を介して接続された制御用プロセッサ８を有し、この制御用プロセッサ８は、ユニット内を制御すると共に、その内部にはローカルなメモリが内蔵されている。この制御用プロセッサ８には、データ送受信用のバス１０を介して、第１ＬＳＩ１２ａ，１２ｂ、記憶装置１４、検索ブロック１６ａ，１６ｂ及び検証用プロセッサ１８が接続されている。

【００１５】第１ＬＳＩ１２ａ，１２ｂは、後述する解読事前処理にて、初期値から表の要素を作成する。記憶装置１４には、上記表等が格納される。検索ブロック１６ａ，１６ｂは、解読処理において値の検索を行う。

【００１６】この検索ブロック１６ａ，１６ｂ内においては、比較プロセッサ２０に第２ＬＳＩ２２及びメモリ２４が接続されている。比較プロセッサ２０は、メモリ２４や第２ＬＳＩ２２を制御して、表の要素の検索を制御する。メモリ２４では、表等を展開する。そして、第２ＬＳＩ２２では、暗号文を加工する。そして、展開された表と、暗号文を加工した値と、を比較プロセッサ２０で比較する。

【００１７】検証用プロセッサ１８では、検索ブロック１６ａ，１６ｂが求めた解の候補を検証する。この検証用プロセッサ１８には、第３ＬＳＩ２６が接続されており、第３ＬＳＩ２６は検証用プロセッサ１８が解の候補を検証する際に、値を加工する。

【００１８】第２ＬＳＩ２２及び第３ＬＳＩ２６に内蔵されている暗号加工回路を図２に示す。図２において、暗号加工回路は、暗号化回路３０と縮退化回路３２とを有する。暗号化回路３０では、入力された値の暗号化が行われる。縮退化回路３２では、暗号化された値が縮退関数によって変形される。なお、これらの回路３０、３２の入力及び出力位置に、２入力１出力のセレクタ３４、３６、３８が配置されている。セレクタ３４は外部からの初期値と内部でループする際の値とを切り替え、セレクタ３６は暗号化の有無を切り替え、セレクタ３８は縮退関数による変形の有無を切り替える。

【００１９】上述のように構成された暗号強度評価装置を使用して解読処理が行われるが、先ず、暗号文の入手前に表を作成する解読前処理について説明する。

【００２０】解読前処理では、以下に示すような手順で各処理が行われる。

【００２１】（１）ローカルコンピュータ２は、ユーザの指示に従い、平文等の処理に必要なパラメータを決定する。

【００２２】（２）ローカルコンピュータ２は、表作成の処理を各ユニット６ａ，６ｂに分配する。この際、ローカルコンピュータ２は平文、作成する表のタイプ（表タイプ番号が例えば１００番から２００番等）、表の要素数Ｍ、表作成のための加工繰り返し回数Ｔ等のパラメータを、ネットワーク４を介して、各ユニット６ａ，６ｂ内の制御用プロセッサ８へ送る。

【００２３】（３）制御用プロセッサ８は平文、表のタイプ、初期値、加工繰り返し回数Ｔ等のパラメータを第１ＬＳＩ１２ａ，１２ｂへ送り、表の要素の作成を指示する。この際、初期値は表のタイプと、作成する要素の表における指標値（ｉｎｄｅｘ番号）から生成する。例えば、初期値は、『表のタイプ番号＜＜ｌｏｇ（Ｍ）＋指標値』の関係を満たす指標値等から作成できる。

【００２４】（４）第１ＬＳＩ１２ａ，１２ｂは、平文及び初期値を入力として、指定された表のタイプに応じた処理を行い、新しい値を生成する。第１ＬＳＩ１２ａ，１２ｂは内部ループを持ち、上記新しい値を初期値の代わりに用いて、更に新しい値を生成する。そして、上述の過程をＴ回数繰り返す。要素作成が終了した場合、第１ＬＳＩ１２ａ，１２ｂは制御用プロセッサ８に終了報告を行う。

【００２５】（５）制御用プロセッサ８は終了報告を受け取った後、（４）でできた値を第１ＬＳＩ１２ａ，１２ｂから取りだし、次の表の要素作成を第１ＬＳＩ１２ａ，１２ｂに指示する。この指示は制御用プロセッサ８の処理が終了するまで繰り返される。

【００２６】（６）制御用プロセッサ８は、表の全ての要素を受け取った場合、バス１０を介して、その表を記

憶装置１４に書き込む。この際、表の各要素から、その作成に用いられた初期値を求めるのに必要な情報も合わせて格納する。これらの処理を全ての表を作成するまで繰り返す。

【００２７】（７）制御用プロセッサ８は全ての表の作成が終了した場合、その旨をローカルコンピュータ２に報告する。

【００２８】（８）ローカルコンピュータ２は全てのユニット６ａ，６ｂから終了報告を受け取るまで待機し、終了報告を受け取った場合、解読前処理は終了する。

【００２９】次に、解読処理についての手順について、以下に説明する。

【００３０】（１）ローカルコンピュータ２に暗号文が、入力される。

【００３１】（２）ローカルコンピュータ２は、暗号文をネットワーク４を介して、各ユニット６ａ，６ｂの制御用プロセッサ８に送る。

【００３２】（３）制御用プロセッサ８は、暗号文を検索ブロック１６ａ，１６ｂに送り、その後記憶装置１４から表を取り出し、各検索ブロック１６ａ，１６ｂに配布する。

【００３３】（４）検索ブロック１６ａ，１６ｂの比較プロセッサ２０は暗号文と表とを受け取ると、それをメモリ２４に格納する。

【００３４】（５）比較プロセッサ２０は第２ＬＳＩ２２に暗号文を入力として加工処理させ、新しい値を取り出し、表の各要素との比較を行う。この際、入力された値（暗号文）は、暗号化回路３０を経由せず、縮退化回路３２の加工処理のみ行われたものが新しい値となる。

【００３５】（６）比較プロセッサ２０は表の要素の中に一致するものがあれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【００３６】（７）比較プロセッサ２０は、新しい値を入力処理させ、さらに新しい値を取り出し、表の各要素との比較を行う。この際、入力された値は、暗号化及び縮退化の両方の加工処理を受けて生成された値となる。

【００３７】（８）解読前処理における加工繰り返し回数Ｔだけ、（６）及び（７）を繰り返す。

【００３８】（９）比較プロセッサ２０は、上記（５）～（８）の処理において、一致する値の有無と、一致する値があった場合における要素に対応する初期値と、（５）の処理を０回目として上記一致した場合の加工処理は何回目の加工処理であるかと、に関する情報を制御用プロセッサ８に報告する。

【００３９】（１０）制御用プロセッサ８は一致した値が報告された場合、その初期値、検索に要した加工回数、平文、表のタイプ番号、表作成時の加工回数Ｔを検証用プロセッサ１８に送る。また、一致した値の有無にかかわらず、記憶装置１４から他の表を取り出し、検索ブロック１６ａ，１６ｂに対して、上記（４）から（１０）の加工処理を行う。そして、記憶装置１４内に記憶されている全ての表に対して、上述の加工処理を行う。

【００４０】（１１）検証用プロセッサ１８は、表作成時に行われた加工回数Ｔから、上記検索に要した加工回数を引いた処理回数値を求め、初期値、平文、表のタイプ番号及び処理回数値を第３ＬＳＩ２６に送る。

【００４１】（１２）第３ＬＳＩ２６は、初期値、平文、表のタイプ番号、処理回数値を受け取り、その値から１を引いた回数だけ加工処理を繰り返した結果と、最後にもう一度加工処理した結果と、を検証用プロセッサ１８に送る。この際、前者は暗号化と縮退化の両方を経由したものであり、後者は暗号化のみを経由したものである。

【００４２】（１３）検証用プロセッサ１８は、第３ＬＳＩ２６から受け取った値のうち、縮退化を経由しなかった値と、暗号文と、を比較する。比較した結果、値が一致した場合、１回分処理の少ない値を解読結果（暗号文の鍵）として、制御用プロセッサ８に報告する。値が一致しなかった場合、終了報告のみを報告する。

【００４３】（１４）制御用プロセッサ８は解読結果を受け取った場合、その値をネットワーク４を介して、ローカルコンピュータ２に報告する。一方、終了報告を受け取った場合には、他の検証すべき値を検証用プロセッサ１８に送る。

【００４４】（１５）制御用プロセッサ８は全ての表の処理が終了した場合、ローカルコンピュータ２に対して、その終了報告を行う。

【００４５】（１６）ローカルコンピュータ２は解読結果（鍵）を受け取った場合、その値を表示すると共に、各ユニット６ａ，６ｂに対し、処理の中止を指示する。また、解読結果を受け取らず、全てのユニット６ａ，６ｂから終了報告を受け取った場合、鍵が発見できなかった旨を表示する。

【００４６】以上の（１）から（１６）の処理により、解読処理は終了する。

【００４７】以上のようにして、実施の形態１に示された装置により、従来の暗号強度評価方法を実現することができる。

【００４８】実施の形態２．本発明の実施の形態２である暗号強度評価装置において、実施の形態１である暗号強度評価装置と異なる点は、比較プロセッサ２０により、メモリ２４に格納される表が異なる点にあり、必要な構成要素は実施の形態１と同一である。

【００４９】実施の形態１では、比較プロセッサ２０は第２ＬＳＩ２２から受け取った値と、表の各要素と、の比較をそのまま行っていた。このため、表の要素から初期値を求めるための変換テーブルのようなものが必要となる。そこで、実施の形態２では、実施の形態１の解読処理（４）でメモリ２４に表を格納する際に、ソートやハッシュをおこなう。これにより、上記変換テーブルの

情報が付加された表がメモリ２４に格納されて、比較時間を短縮することができる。上記ハッシュとしては、表の要素数をＭとし、下位ｌｏｇ（Ｍ）ビットをハッシュ関数として取り出してアドレスとする方法や、事前に数ビットシフトしてから上記方法と同様に下位ビットをハッシュ関数として取り出す方法等がある。なお、ハッシュにおける値の衝突については、衝突したものをチェーンリストで実装する方法、衝突の際に２つめ以降の値を無視する方法、衝突のある表自体を無視する方法等により、衝突の影響を回避できる。

【００５０】実施の形態３．本発明の実施の形態３である暗号強度評価装置において、実施の形態２で示された装置と異なる点を以下に示す。実施の形態２では、解読処理（４）で表をメモリ２４に格納する際に、ソートやハッシュを行ってから、メモリ２４に格納していたが、本実施の形態では、解読前処理（６）の時点でソートやハッシュが行われ、この表が、記憶装置１４に格納されている。この場合におけるソートやハッシュの仕方について、以下に示す。

【００５１】（６１）制御用プロセッサ８は表の値を比較プロセッサ２０へ送る。

【００５２】（６２）比較プロセッサ２０は表の値をメモリ２４に展開し、これにソートやハッシュの変換処理を行う。そして、変換テーブルを含む表を作成して、これを制御用プロセッサ８に送る。

【００５３】（６３）制御用プロセッサ８は、受け取った新たな表の値を記憶装置１４に格納する。このため、変換テーブル分、記憶装置１４に必要な容量が増える。

【００５４】そして、解読処理の際には、記憶装置１４から表を取り出して、各処理をすることができる。

【００５５】実施の形態３において、事前に数ビットシフトしてから下位ビットを取り出すハッシュを行う場合、シフトするビット数を調整することで、高い確率でハッシュ値の衝突を避けることができる。また、解読処理前に行っているため、衝突が避けられない表は削除し、別の表タイプ番号の表を作成（追加）することも可能である。

【００５６】実施の形態４．図１に示すように、実施の形態１の暗号強度評価装置では、制御用プロセッサ８と検証用プロセッサ１８とを別々のものにしていたが、本実施の形態では、制御用プロセッサ８が検証用プロセッサ１８の検証機能を有する。このため、検証用プロセッサ１８を省略することができる。この際、第３ＬＳＩ２６は制御用プロセッサ８又はバス１０に接続される。

【００５７】実施の形態５．実施の形態１の暗号強度評価装置では、第１ＬＳＩ１２ａ，１２ｂに１つの初期値を与えて値を生成しているが、本実施の形態では、１つのＬＳＩ１２ａに複数の初期値を与えて処理させる。この際、暗号化回路３０や縮退化回路３２には、その内部に複数のラッチを入れ、回路内の値を保持させ、動作周波数を上げている。

【００５８】本実施の形態５においては、ラッチ分だけ回路規模が大きくなるが、動作周波数を上げることができるので、ＬＳＩ２２，２６のスループットが向上する。

【００５９】実施の形態６．実施の形態６における暗号強度評価装置では、実施の形態１で別々のものであった第１ＬＳＩ１２ａ，１２ｂと第２ＬＳＩ２２とを、１つのＬＳＩにまとめている。

【００６０】これにより、例えば解読前処理も第２ＬＳＩ２２に行わせることで、第１ＬＳＩ１２ａ，１２ｂを省略することができる。但し、第１ＬＳＩ１２ａ，１２ｂに要求されている性能はスループット性能であり、第２ＬＳＩ２２に要求されている性能はレイテンシィ性能である。また、解読前処理と、解読処理と、では処理量が異なる。このため、第１ＬＳＩ１２ａ，１２ｂと第２ＬＳＩ２２とを、共用させる範囲には制限がある。また、第３ＬＳＩ２６も第２ＬＳＩ２２と共用させることが可能である。

【００６１】実施の形態７．本実施の形態の暗号強度評価装置において、実施の形態１で示す暗号強度評価装置と異なる点は、メモリ２４を連想記憶メモリにしている点にある。そして、連想記憶メモリが第２ＬＳＩ２２の出力値と表の要素とが一致したと判定した場合には、その値を取り出す回路で、比較プロセッサ２０は構成されている。

【００６２】これにより、実施の形態２で行われている表変換を行うことなく、第２ＬＳＩ２２の出力値の値と表の要素とが一致した場合には、ほぼ一定時間でそのアドレスを知ることができる。なお、表が１つの連想記憶メモリに格納できない場合には、比較プロセッサ２０は、複数の連想記憶メモリに表を分割して格納し、第２ＬＳＩ２２の出力結果を各連想記憶メモリにブロードキャストすることで一致する値を探索する。

【００６３】実施の形態８．本実施の形態の暗号強度評価装置において、実施の形態１で示す暗号強度評価装置と異なる点は、メモリ２４を連想記憶メモリにすると共に、比較プロセッサ２０の機能を第２ＬＳＩ２２に埋め込んでいる点にある。

【００６４】実施の形態７では比較プロセッサ２０は、連想記憶メモリに第２ＬＳＩ２２の出力値を送る。そして、この値と表の要素とが一致した場合には、比較プロセッサ２０は、その信号とアドレスとを受け取り、制御用プロセッサ８に報告しているだけである。このため、比較プロセッサ２０を実現する回路は、比較的単純であり、第２ＬＳＩ２２に埋め込むことができる。

【００６５】実施の形態９．本実施の形態の暗号強度評価装置では、暗号化回路３０について、ＤＥＳ暗号に暗号化する回路から、例えばＦＥＡＬ暗号に暗号化する回路に変更することが可能である。このため、強度評価す

る暗号に応じて、暗号化回路３０を変更すれば、どの暗号に対しても、暗号強度評価を行うことができる。

【００６６】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、従来で行われた暗号強度評価方法を行うことができる装置を実現することができる。

【００６７】請求項２に記載の発明によれば、複数種のＬＳＩを１つのＬＳＩにまとめることにより、装置内の部品点数を減らすことができ、装置の小型化を図ることができる。また、１つのＬＳＩを開発すればよいので、その開発コストを低減できる。

【００６８】請求項３に記載の発明によれば、連想記憶メモリを使用することで、ハッシュ等の処理を行わなくとも、短時間で、表の要素と暗号文の加工値とを比較することができる。

【００６９】請求項４に記載の発明によれば、第２ＬＳＩに比較プロセッサが有する機能の回路を付加することにより、比較プロセッサを省略することができる。この

ため、装置の小型化を図ることができる。

【００７０】請求項５に記載の発明によれば、各ＬＳＩを装置が強度評価する暗号に対応するように設定できるので、どの暗号に対しても、暗号強度評価を行うことができる。

【図面の簡単な説明】

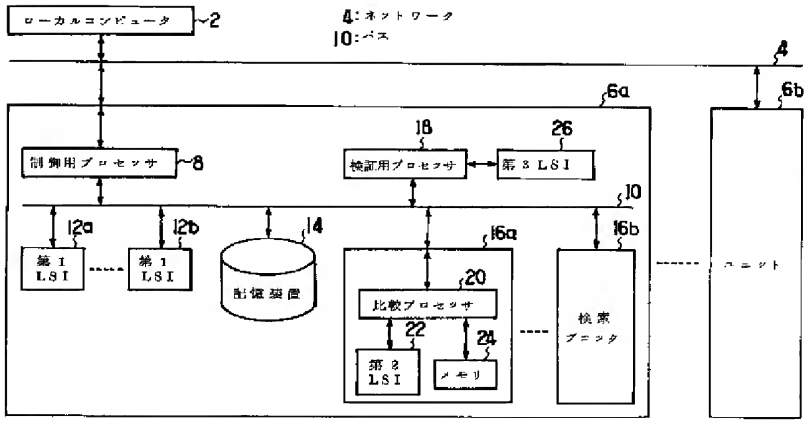
【図１】　本発明の実施の形態である暗号強度評価装置を示すブロック図である。

【図２】　本発明の実施の形態である暗号加工回路を示すブロック図である。

【符号の説明】

２　ローカルコンピュータ、４　ネットワーク、６ａ，６ｂ　ユニット、８制御用プロセッサ、１０　バス、１２ａ，１２ｂ　第１ＬＳＩ、１４　記憶装置、１６ａ，１６ｂ　検索ブロック、１８　検証用プロセッサ、２０　比較プロセッサ、２２　第２ＬＳＩ、２４　メモリ、３０　暗号化回路、３２　縮退化回路、３４，３６，３８　セレクタ。

【図１】



【図２】